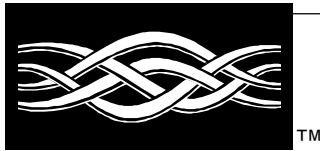




Microsoft®

Microsoft®
Windows NT® Server

Server Operating System



White Paper

Understanding Point-to-Point Tunneling Protocol (PPTP)

Microsoft® **Windows NT® Server**

Understanding PPTP

Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables the secure transfer of data from a remote client to a private enterprise server by creating a virtual private network (VPN) across TCP/IP-based data networks. PPTP supports on-demand, multi-protocol, virtual private networking over public networks, such as the Internet.

© 1997 Microsoft Corporation. All rights reserved.

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This White Paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Microsoft, Windows, and Windows NT are registered trademarks and BackOffice and the BackOffice logo are trademarks of Microsoft Corporation.

Other product or company names mentioned herein may be the trademarks of their respective owners.

Microsoft Corporation • One Microsoft Way • Redmond, WA 98052-6399 • USA

0197 Part no. 098-68564

CONTENTS

INTRODUCTION	1
PPTP AND VIRTUAL PRIVATE NETWORKING	2
Typical PPTP Scenario	2
PPTP Clients	4
Network Access Servers at an ISP	5
PPTP Servers on the Private LAN	6
PPTP ARCHITECTURE	7
PPTP Architecture Overview	7
PPP Protocol	7
PPTP Control Connection	8
PPTP Data Transmission	10
UNDERSTANDING PPTP SECURITY	11
Authentication	11
Access Control	12
Data Encryption	12
PPTP Packet Filtering	12
Using PPTP with Firewalls and Routers	13

INTRODUCTION

Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables the secure transfer of data from a remote client to a private enterprise server by creating a virtual private network (VPN) across TCP/IP-based data networks. PPTP supports on-demand, multi-protocol, virtual private networking over public networks such as the Internet.

The networking technology of PPTP is an extension of the remote access Point-to-Point protocol defined in the document by the Internet Engineering Task Force (IETF) titled "The Point-to-Point Protocol for the Transmission of Multi-Protocol Datagrams over Point-to-Point Links," referred to as RFC 1171. PPTP is a network protocol that encapsulates PPP packets into IP datagrams for transmission over the Internet or other public TCP/IP-based networks. PPTP can also be used in private LAN-to-LAN networking.

The PPTP extension of PPP is explained in the document titled "Point-to-Point Tunneling Protocol," PPTP draft-ietf-ppext-pptp-00.Text. A draft of this document was submitted to the IETF in June, 1996 by the companies of the PPTP Forum, which includes Microsoft Corporation, Ascend Communications, 3Com/Primary Access, ECI Telematics, and US Robotics.

Note

Internet draft documents should be considered as a "works in progress." See www.ietf.org for copies of Internet drafts and RFCs mentioned in this document. For more information about PPTP, visit our Web site at <http://www.microsoft.com/ntserver>. See the topic "Network Communications and Telephony" under "All About..."

This document is for network administrators, support personnel, and developers who need to understand how PPTP can be used to provide low-cost remote access solutions and includes the following topics:

- PPTP and secure, virtual private networking (VPN)
- architecture of PPTP
- PPTP security features

PPTP AND VIRTUAL PRIVATE NETWORKING

The PPTP protocol is included with Windows NT® Server version 4.0 and Windows NT Workstation version 4.0 operating systems. Computers running these operating can use the PPTP protocol to securely connect to a private network as a remote access client by using a public data network such as the Internet. In other words, PPTP enables on-demand, virtual private networks over the Internet or other public TCP/IP-based data networks. PPTP can also be used by computers connected to a LAN to create a virtual private network across the LAN.

An important feature in the use of PPTP is its support for virtual private networking by using public-switched telephone networks (PSTNs). PPTP simplifies and reduces the cost of deploying an enterprise-wide, remote access solution for remote or mobile users because it provides secure and encrypted communications over public telephone lines and the Internet. PPTP eliminates the need for expensive, leased-line or private enterprise-dedicated communication servers because you can use PPTP over PSTN lines. Generally, there are three computers involved in every PPTP deployment:

- a PPTP client
- a network access server
- a PPTP server

Note

You do not need the network access server in order to create a PPTP tunnel when using a PPTP client connected to a LAN to connect to a PPTP server connected to the same LAN.

The following section describes a typical PPTP scenario using these computers and explains how they relate to each other and then fully defines each of these components.

Typical PPTP Scenario

A typical deployment of PPTP starts with a remote or mobile PPTP client that needs access to a private enterprise LAN by using a local Internet Service Provider (ISP). Clients using computers running Windows NT Server version 4.0 or Windows NT Workstation version 4.0 use Dial-up Networking and the remote access protocol PPP to connect to an ISP.

The client connects to a network access server (NAS) at the ISP facility. (Network access servers are also referred to as front-end processors (FEPs), dial-in servers or point-of-presence (POP) servers.) Once connected, the client can send and receive packets over the Internet. The network access server uses the TCP/IP protocol for all traffic to the Internet.

After the client has made the initial PPP connection to the ISP, a second Dial-Up Networking call is made over the existing PPP connection. Data sent using this second connection is in the form of IP datagrams that contain PPP packets, referred to as encapsulated PPP packets.

The second call creates the virtual private networking (VPN) connection to a PPTP server on the private enterprise LAN, this is referred to as a *tunnel*. This is shown in the following figure:

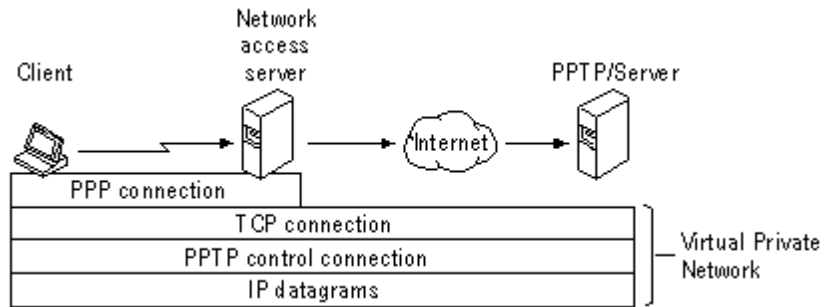


Figure 1 - The PPTP Tunnel

Tunneling is the process of sending packets to a computer on a private network by routing them over some other network, such as the Internet. The other network routers cannot access the computer that is on the private network. However, tunneling enables the routing network to transmit the packet to an intermediary computer, such as a PPTP server, that is connected to the both the routing network and the private network. Both the PPTP client and the PPTP server use tunneling to securely route packets to a computer on the private network by using routers that only know the address of the private network intermediary server.

When the PPTP server receives the packet from the routing network, it sends it across the private network to the destination computer. The PPTP server does this by processing the PPTP packet to obtain the private network computer name or address information in the encapsulated PPP packet. Note that the encapsulated PPP packet can contain multi-protocol data such as TCP/IP, IPX, or NetBEUI protocols. Because the PPTP server is configured to communicate across the private network by using private network protocols, it is able to read multi-protocol packets.

The following figure illustrates the multi-protocol support built-into PPTP. A packet sent from the PPTP client to the PPTP server passes through the PPTP tunnel to a destination computer on the private network.

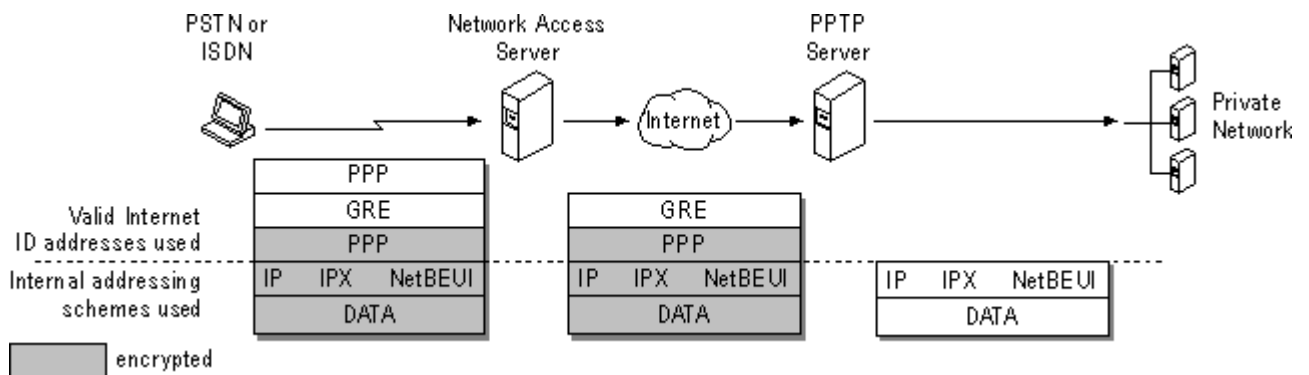


Figure 2 - Connecting a Dial-Up Networking PPTP Client to the Private Network

PPTP encapsulates the encrypted and compressed PPP packets into IP datagrams for transmission over the Internet. These IP datagrams are routed over the Internet until they reach the PPTP server that is connected to the

Internet and the private network. The PPTP server disassembles the IP datagram into a PPP packet and then decrypts the PPP packet using the network protocol of the private network. As mentioned earlier, the network protocols on the private network that are supported by PPTP are IPX, NetBEUI, or TCP/IP.

PPTP Clients

A computer that supports the PPTP network protocol, e.g., a Microsoft client, can connect to a PPTP server in two ways:

- by using an ISP's network access server that supports inbound PPP connections
- by using a physical TCP/IP-enabled LAN connection to connect to a PPTP server

PPTP clients that use an ISP's network access server must be configured with a modem and a VPN device to make the separate connections to the ISP and the PPTP server. The first connection is a dial-up connection using the PPP protocol over the modem to an Internet service provider. The second connection is a VPN connection using PPTP, over the modem and the ISP connection, to tunnel across the Internet to a VPN device on the PPTP server. The second connection requires the first connection because the tunnel between the VPN devices is established by using the modem and PPP connection to the Internet.

The exception to this two-connection requirement is using PPTP to create a virtual private network between computers physically connected to the private enterprise network LAN. In this scenario, a PPTP client is already connected to the network and only uses Dial-Up Networking with a VPN device to create the connection to a PPTP server on the LAN.

PPTP packets from a remote access PPTP client and a local LAN PPTP client are processed differently. A PPTP packet from a remote access PPTP client is placed on the telecommunication device physical media, while the PPTP packet from a LAN PPTP client is placed on the network adapter physical media as illustrated in the following figure:

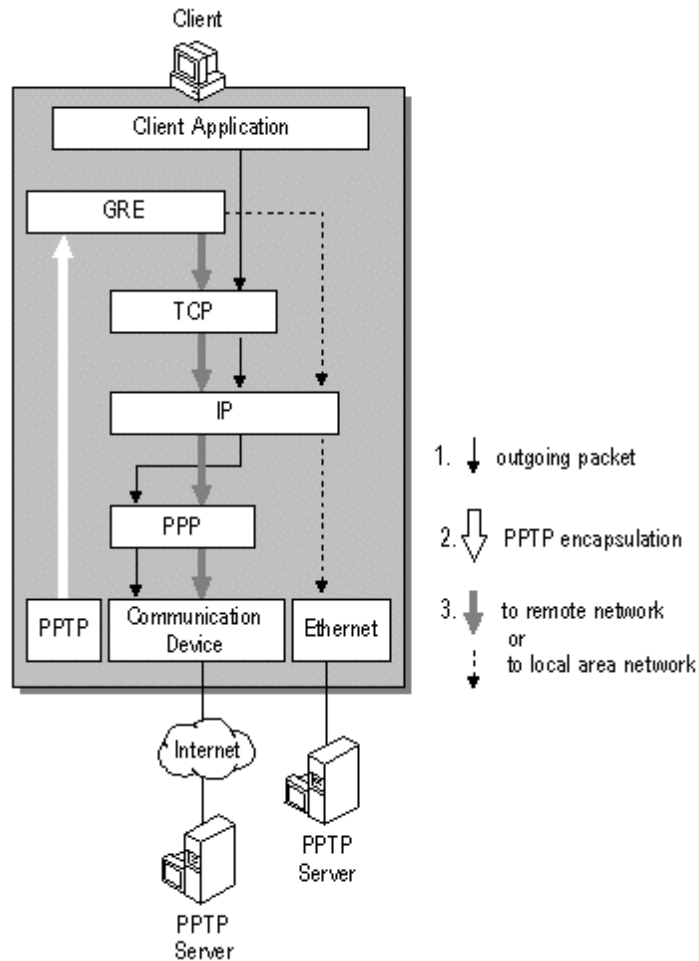


Figure 3 - Placing a PPTP packet on the Network Media

The figure above illustrates how PPTP encapsulates PPP packets and then places the outgoing PPTP packet on either a modem, ISDN, or LAN network media.

Network Access Servers at an ISP

ISPs use network access servers to support clients that dial in using a protocol, such as SLIP or PPP, to gain access to the Internet. However, to support PPTP-enabled clients, a network access server must provide PPP service.

The ISP network access servers are designed and built to accommodate a high number of dial-in clients. Network access servers are built by companies such as 3Com, Ascend, ECI Telematics, and U.S. Robotics, that are members of the PPTP Forum.

Note

An ISP that provides a PPTP service by using a PPTP-enabled network access server can support Windows+ 95, Windows NT versions 3.5 and 3.51, as well as third-party PPP clients, such as Apple Macintosh or UNIX. These clients can use a PPP connection to the ISP server. The ISP server acts as a PPTP client

and connects to the PPTP server on the private network, creating a PPTP tunnel from the ISP server to the PPTP server.

In this scenario, the PPTP architecture described in this document is fundamentally the same; however, all PPTP communication occurs between the network access server and PPTP server. Contact your ISP to see if they provide a PPTP service and how you need to configure PPP and Dial-Up Networking to access the ISP server that supports PPTP.

PPTP Servers on the Private LAN

PPTP servers are servers with routing capabilities that are connected to a private network and to the Internet. In this document, a PPTP server defined as a computer running Windows NT Server version 4.0 and RAS. PPTP is installed as a network protocol. During installation, PPTP is configured by adding virtual devices referred to as *virtual private networks* (VPNs) to the RAS and Dial-Up Networking. For more information about PPTP server installation requirements, see the document "Using PPTP."

PPTP ARCHITECTURE

This section provides information about the architecture of PPTP under Windows NT Server version 4.0 or Windows NT Workstation version 4.0. PPTP is designed to provide a secure method for reaching private networks over the Internet. Examining the PPTP reveals the secure design features of the PPTP protocol.

This section describes:

- PPP protocol
- PPTP control connection
- PPTP data tunneling

PPTP Architecture Overview

The secure communication created using the PPTP protocol typically involves three processes, each of which requires successful completion of the previous process. This document explains these three processes and how they work:

PPP Connection and Communication. A PPTP client uses PPP to connect to an ISP by using a standard telephone line or ISDN line. This connection uses the PPP protocol to establish the connection and encrypt data packets.

PPTP Control Connection. Using the connection to the Internet established by the PPP protocol, the PPTP protocol creates a control connection from the PPTP client to a PPTP server on the Internet. This connection uses TCP to establish the connection and is called a PPTP *tunnel*.

PPTP Data Tunneling. Finally, the PPTP protocol creates IP datagrams containing encrypted PPP packets which are then sent through the PPTP tunnel to the PPTP server. The PPTP server disassembles the IP datagrams and decrypts the PPP packets, and then routes the decrypted packets to the private network.

PPP Protocol

PPP is a remote access protocol used by PPTP to send multi-protocol data across TCP/IP-based networks. PPP encapsulates IP, IPX, and NetBEUI packets between PPP frames and sends the encapsulated packets by creating a point-to-point link between the sending and receiving computers.

Most PPTP sessions are started by a client dialing up an ISP network access server. The PPP protocol is used to create the dial-up connection between the client and network access server and performs the following three functions:

- **Establishes and ends the physical connection.** The PPP protocol uses a sequence defined in RFC 1661 to establish and maintain connections between remote computers.
- **Authenticates users.** PPTP clients are authenticated by using the PPP protocol. Clear text, encrypted, or Microsoft encrypted authentication can be used by the PPP protocol.
- **Creates PPP datagrams that contain encrypted IPX, NetBEUI, or TCP/IP packets.** PPP creates datagrams which contain one or more encrypted TCP/IP, IPX, or NetBEUI data packets. Because the network packets are encrypted, all traffic between a PPP client and a network

access server is secure.

This entire process is illustrated in the following illustration.

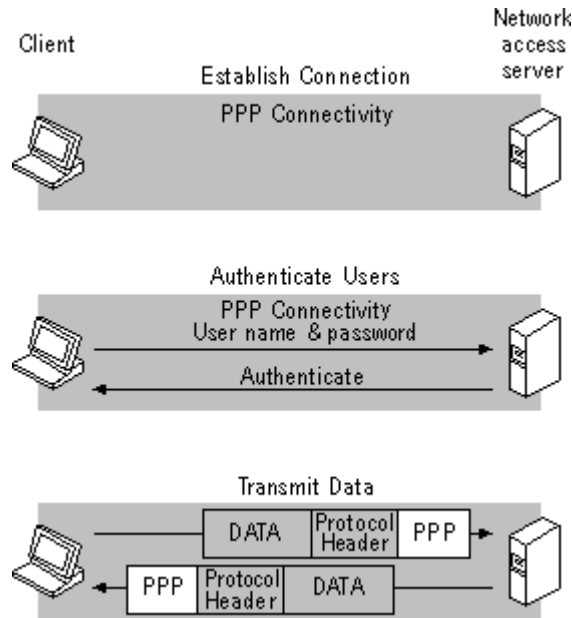


Figure 4 - Dial-Up Networking PPP Connection to ISP

Note

In some situations, remote clients may have direct access to a TCP/IP network, such as the Internet. For example, a laptop computer with a network card can use an Internet tap in a conference room. With a direct IP connection, the initial PPP connection to an ISP is unnecessary. The client can initiate the connection to the PPTP server, without first making a PPP connection to an ISP.

PPTP Control Connection

The PPTP protocol specifies a series of control messages sent between the PPTP-enabled client and the PPTP server. The control messages establish, maintain and end the PPTP tunnel. The following list presents the primary control messages used to establish and maintain the PPTP tunnel.

Message Type	Purpose
PPTP_START_SESSION_REQUEST	Starts Session
PPTP_START_SESSION_REPLY	Replies to start session request
PPTP_ECHO_REQUEST	Maintains session
PPTP_ECHO_REPLY	Replies to maintain session request
PPTP_WAN_ERROR_NOTIFY	Reports an error on the PPP connection
PPTP_SET_LINK_INFO	Configures the connection between client and PPTP Server
PPTP_STOP_SESSION_REQUEST	Ends session
PPTP_STOP_SESSION_REPLY	Replies to end session request

Table 1 - PPTP Control Message Types

Control messages are transmitted in control packets in a TCP datagram. One TCP connection is created between the PPTP client and the PPTP server. This connection is used to exchange control messages. The control messages are sent in TCP datagrams containing the control messages. A datagram contains a PPP header, a TCP header, a PPTP control message, and appropriate trailers, similar to the following:

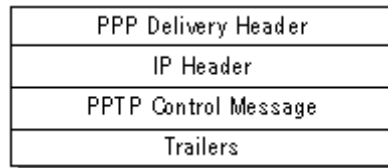


Figure 5 - PPTP TCP Datagram with Control Messages

The exchange of messages between the PPTP client and the PPTP server over the TCP connection are used to create and maintain a PPTP tunnel. This entire process is illustrated below:

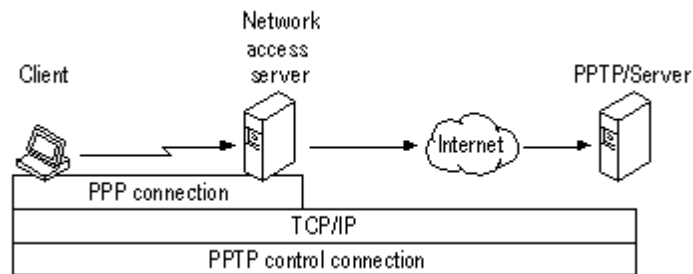


Figure 6 - PPTP Control Connection to PPTP Server Over PPP Connection to ISP

Note that in this illustration, the control connection is for the scenario in which the remote access client is the PPTP client. In the scenario in which the remote access client is not PPTP-enabled and uses a PPTP-enabled ISP network

access server, the PPTP control connection begins at the ISP server. For detailed information about the PPTP protocol and its control connection messages and TCP datagram construction, see the PPTP Internet draft.

PPTP Data Transmission

After the PPTP tunnel is established, user data is transmitted between the client and PPTP server. Data is transmitted in IP datagrams containing PPP packets. The IP datagrams are created using a modified version of the Internet Generic Routing Encapsulation (GRE) protocol. (GRE is defined in RFCs 1701 and 1702.) The IP datagram created by PPTP is similar to the following:

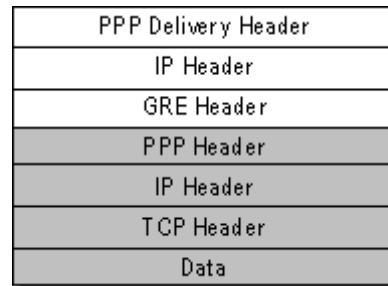


Figure 7 - IP datagram Containing Encrypted PPP packet as created by PPTP

The IP delivery header provides the information necessary for the datagram to traverse the Internet. The GRE header is used to encapsulate the PPP packet within the IP datagram. The PPP packet was created by RAS. Note that the PPP packet is just one unintelligible block because it is encrypted. Even if the IP datagram were intercepted, it would be nearly impossible to decrypt the data.

UNDERSTANDING PPTP SECURITY

PPTP extends the strict authentication and encryption security available to computers running RAS under Windows NT Server version 4.0 and Windows NT Workstation version 4.0 to PPTP clients on the Internet. PPTP also can protect the PPTP server and private network by ignoring all but PPTP traffic. Despite the strict security, it is very simple to use PPTP with existing firewalls. This section will help you understand and plan the following:

- authentication and access control
- data encryption
- PPTP packet filtering
- using third-party firewalls

Authentication

Initial dial-in authentication may be required by an ISP network access server. If this authentication is required, it is strictly to log on to the ISP network access server; it is not related to Windows NT-based authentication. Check with your ISP for their authentication requirements. You apply these requirements in the Dial-Up Networking entry for that ISP.

On the other hand, if the Windows NT Server version 4.0 is configured as a PPTP server, it controls all access to your private network. That is, the PPTP server is a gateway to your private network. The PPTP server requires a standard Windows NT-based logon. All PPTP clients must supply a user name and password. Therefore, remote access logon using a computer running under Windows NT Server version 4.0 or Windows NT Workstation version 4.0 is as secure as logging on from a Windows NT-based computer connected to the local LAN.

Authentication of remote PPTP clients is done by using the same PPP authentication methods used for any RAS client dialing directly to a RAS server. Microsoft's implementation of the Remote Access Service (RAS) supports the Challenge Handshake Authentication Protocol (CHAP), the Microsoft Challenge Handshake Authentication Protocol (MS-CHAP), and the Password Authentication Protocol (PAP) authentication schemes.

Note

MS-CHAP authentication supports the MD4 hash as well as the earlier authentication scheme used in Microsoft LAN Manager.

As with all user accounts, the user accounts of remote users reside in the Windows NT Server version 4.0 directory service and are administered through User Manager for Domains. This provides centralized administration that is integrated with the private network's existing user accounts. Only accounts that have been granted specific access to the network through a trusted domain are permitted. Careful user accounts management is necessary to reduce security risks.

Having a secure password model in place is critical to successful deployment of PPTP because Internet connections are more susceptible to speed or "demon dialer" programs, which can literally crunch through thousands of password and username combinations.

The only way to minimize this type of attack is to implement secure password policies. Passwords should be difficult to guess. For example, you can require passwords to contain upper case letters, lower case letters, numbers, and special characters. It is recommended you require at least three different types of characters to ensure password uniqueness.

Access Control

After authentication, all access to a private LAN continues to use the Windows NT-based security model. Access to resources on NTFS drives, or to other network resources require the proper permissions. It is recommended that the NTFS file system is used for file resources that are accessed by PPTP clients.

For more information about using security on NTFS drives or other network resources, see your product documentation or the Windows NT Workstation version 4.0 and Windows NT Server version 4.0 Resource Kits.

Data Encryption

For data encryption, PPTP uses the RAS "shared-secret" encryption process. It is referred to as a shared-secret because both ends of the connection share the encryption key. Under the Microsoft implementation of RAS, the shared secret is the user password. (Other encryption methods base the encryption on some key available in public; this second method of encryption is known as *public key encryption*.)

PPTP uses the PPP encryption and PPP compression schemes. The CCP (Compression Control Protocol) used by PPP is used to negotiate encryption.

The user name and password of the PPTP client is available to the PPTP server and supplied by the PPTP client. An encryption key is derived from the hashed password stored on both the client and server. The RSA RC4 standard is used to create this 40-bit session key based on the client password. This key is used to encrypt all data that is passed over the Internet, keeping the remote connection private and secure.

The data in PPP packets is encrypted. The PPP packet containing a block of encrypted data is then encapsulated into a larger IP datagram for routing over the Internet to the PPTP server. If an Internet hacker intercepted your IP datagram, he or she would find only media headers, IP headers, and then the PPP packet containing a block of encrypted data. It would be indecipherable.

Note

Users in the United States and Canada can obtain a 128-bit session key through a cryptography pack for use inside the US. Contact your Microsoft reseller for more information.

PPTP Packet Filtering

Network security from malicious activity can be enhanced by enabling PPTP filtering on the PPTP server. When PPTP filtering is enabled, the PPTP server on the private network accepts and routes only PPTP packets from

authenticated users. This prevents **all** other packets from entering the PPTP server and private network. In conjunction with PPP encryption, this ensures that only authorized encrypted data enters or leaves the private LAN.

PPTP filtering is enabled on the PPTP server using the Protocols tab in the Network option of Control Panel. For step-by-step instruction on enabling PPTP filtering, see the white paper titled "Microsoft Point-to-Point Tunneling Protocol".

Using PPTP with Firewalls and Routers

PPTP traffic uses TCP port 1723, and IP protocol uses ID 47, as assigned by the Internet Assigned Numbers Authority (IANA). PPTP can be used with most firewalls and routers by enabling traffic destined for port 1723 to be routed through the firewall or router.

Firewalls ensure corporate network security by strictly regulating data that comes **into** the private network from the Internet. An organization can deploy a PPTP server running Windows NT Server version 4.0 behind its firewall. The PPTP server accepts PPTP packets passed to the private network from the firewall and extracts the PPP packet from the IP datagram, decrypts the packet, and forwards the packet to the computer on the private network.